IN THE CLAIMS

Amended claims follow:

1. (Currently Amended) A computer program product for controlling a computer to execute a computer program within a computer memory, said computer program product comprising:

(a) a loader program; and

(b) an encrypted version of said computer program; wherein said loader program is operable to:

(i) read said encrypted version of said computer program stored in a program store;

(ii) decrypt said encrypted version of said computer program to form said computer program in an executable form;

(iii) load said computer program directly into said computer memory; and

(iv) trigger execution of said computer program as loaded into said computer memory by said loader program;

wherein said computer program that is decrypted, loaded, and executed includes a malware scanning computer program;

wherein said malware scanning computer program is operable such that once executed, said malware scanning computer program scans said loader program for malware;

wherein, if said loader program is detected as being infected with said malware, then said malware scanning computer program is operable to repair said loader program or replace said loader program with a clean copy of said loader program;

wherein said malware scanning computer program is operable to scan for said malware including one or more of a computer virus, a worm, a Trojan, a banned computer file, a banned word and a banned image.

2. (Original) A computer program product as claimed in claim 1, wherein said encrypted version of said computer program is encrypted with a private encryption key

and said loader program is operable to decrypt said encrypted version of said computer program with a corresponding public key.

3. (Original) A computer program product as claimed in claim 1, wherein said encrypted version of said computer program and said loader program are stored as separate computer files within a computer file store.

4. (Original) A computer program product as claimed in claim 1, wherein said loader program is associated with initialisation data specifying one or more of:

a storage location of said encrypted version of said computer program;

a key to be used in decrypting said encrypted version of said computer program; and

parameters specifying how said computer program should be loaded into said computer memory for execution.

5. (Cancelled)

6. (Cancelled)

7. (Cancelled)

8. (Cancelled)

9. (Original) A computer program product as claimed in claim 1, wherein said loader program is operable to terminate after triggering execution of said computer program.

10. (Original) A computer program product as claimed in claim 1, wherein said computer program is operable to terminate said loader program when said computer program is triggered to execute by said loader program.

11. (Original) A computer program product as claimed in claim 1, wherein said loader program is operable to load said computer program into a memory space within said computer memory separate from a memory space used by said loader program.

12. (Original) A computer program product as claimed in claim 1, wherein said loader program is operable to load said computer program into an execution stream separate from an execution stream used by said loader program.

13. (Currently Amended) A method of executing of a computer program within a computer memory, said method comprising the steps of:

(a) executing a loader program, said loader program operating to:

(i) read an encrypted version of said computer program stored in a program store;

(ii) decrypt said encrypted version of said computer program to form said computer program in an executable form;

(iii) load said computer program directly into said computer memory; and

(iv) trigger execution of said computer program; and

(b) executing said computer program as loaded into said computer memory by said loader program;

wherein said computer program that is decrypted, loaded, and executed includes a malware scanning computer program;

wherein said malware scanning computer program is operable such that once executed, said malware scanning computer program scans said loader program for malware;

wherein, if said loader program is detected as being infected with said malware, then said malware scanning computer program is operable to repair said loader program or replace said loader program with a clean copy of said loader program;

wherein said malware scanning computer program is operable to scan for said malware including one or more of a computer virus, a worm, a Trojan, a banned computer file, a banned word and a banned image.

14. (Original) A method as claimed in claim 13, wherein said encrypted version of said computer program is encrypted with a private encryption key and said loader program decrypts said encrypted version of said computer program with a corresponding public key.

15. (Original) A method as claimed in claim 13, wherein said encrypted version of said computer program and said loader program are stored as separate computer files within a computer file store.

16. (Original) A method as claimed in claim 13, wherein said loader program is associated with initialisation data specifying one or more of:

a storage location of said encrypted version of said computer program;

a key to be used in decrypting said encrypted version of said computer program; and

parameters specifying how said computer program should be loaded into said computer memory for execution.

17. (Cancelled)

18. (Cancelled)

19. (Cancelled)

20. (Cancelled)

21. (Original) A method as claimed in claim 13, wherein said loader program terminates after triggering execution of said computer programs.

22. (Original) A method as claimed in claim 13, wherein said computer program terminates said loader program when said computer program is triggered to execute by said loader program.

23. (Original) A method as claimed in claim 13, wherein said loader program loads said computer program into a memory space within said computer memory separate from a memory space used by said loader program.

24. (Original) A method as claimed in claim 13, wherein said loader program loads said computer program into an execution stream separate from an execution stream used by said loader program.

25. (Currently Amended) Apparatus for executing a computer program within a computer memory, said apparatus comprising:

(a) loader program logic; and

(b) a program store operable to store an encrypted version of said computer program;

wherein said loader program logic is operable to:

(i) read said encrypted version of said computer program stored in said program store;

(ii) decrypt said encrypted version of said computer program to form said computer program in an executable form;

(iii) load said computer program directly into said computer memory; and

(iv) trigger execution of said computer program as loaded into said computer memory by said loader program;

wherein said computer program that is decrypted, loaded, and executed includes a malware scanning computer program;

wherein said malware scanning computer program is operable such that once executed, said malware scanning computer program scans said loader program for malware;

wherein, if said loader program is detected as being infected with said malware, then said malware scanning computer program is operable to repair said loader program or replace said loader program with a clean copy of said loader program;

wherein said malware scanning computer program is operable to scan for said malware including one or more of a computer virus, a worm, a Trojan, a banned computer file, a banned word and a banned image.

26. (Original) Apparatus as claimed in claim 25, wherein said encrypted version of said computer program is encrypted with a private encryption key and said loader program logic is operable to decrypt said encrypted version of said computer program with a corresponding public key.

27. (Original) Apparatus as claimed in claim 25, wherein said encrypted version of said computer program and said loader program are stored as separate computer files within a computer file store.

28. (Original) Apparatus as claimed in claim 25, wherein said loader program logic is associated with initialisation data specifying one or more of:

a storage location of said encrypted version of said computer program;

a key to be used in decrypting said encrypted version of said computer program; and

parameters specifying how said computer program should be loaded into said computer memory for execution.

29. (Cancelled)

30. (Cancelled)

31. (Cancelled)

32. (Cancelled)

33. (Original) Apparatus as claimed in claim 25, wherein said loader program logic is operable to terminate after triggering execution of said computer programs.

34. (Original) Apparatus as claimed in claim 25, wherein said computer program logic is operable to terminate said loader program when said computer program is triggered to execute by said loader program.

35. (Original) Apparatus as claimed in claim 25, wherein said loader program logic is operable to load said computer program into a memory space within said computer memory separate from a memory space used by said loader program logic.

36. (Original) Apparatus as claimed in claim 25, wherein said loader program logic is operable to load said computer program into an execution stream separate from an execution stream used by said loader program logic.

37. (New) A computer program product as claimed in claim 1, wherein, as a first task, said malware scanning computer program scans said loader program for said malware.

38. (New) A computer program product as claimed in claim 1, wherein, if said loader program is detected as being infected with said malware, then said malware scanning computer program is operable to replace said loader program with a clean copy of said loader program.

39. (New) A computer program product as claimed in claim 1, wherein, if said loader program is detected as being infected with said malware, then said malware scanning computer program is operable to repair said loader program.